



*Children and adults are at the heart of our school;  
our school is at the heart of our community.*

## **Online Safety policy**

## Contents

1. Aims.....	3
2. Legislation and guidance .....	3
3. Roles and responsibilities .....	3
4. Educating pupils about online safety .....	6
5. Educating parents about online safety .....	6
6. Cyber-bullying.....	6
7. Acceptable use of the internet in school.....	7
8. Pupils using mobile devices in school .....	7
9. Staff using work devices outside school.....	7
10. How the school will respond to issues of misuse .....	7
11. Training.....	7
12. Monitoring arrangements .....	8
13. Links with other policies .....	8
Appendix 1: acceptable use agreement (EYFS and Key Stage 1).....	9
Appendix 2: acceptable use agreement (Key Stage 2).....	10
Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors).....	11
Appendix 4: online safety incident report log .....	<b>Error! Bookmark not defined.</b> 3

.....

## 1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate
- Promote safe use of the internet and digital devices, to enhance learning and promote creativity

## 2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools on:

- › [Teaching online safety in schools](#)
- › [Preventing and tackling bullying](#) and [cyber-bullying: advice for headteachers and school staff](#)
- › [Relationships and sex education](#)
- › [Searching, screening and confiscation](#)

It also refers to the Department's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#) and the [Equality Act 2010](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the [National Curriculum computing programmes of study](#).

## 3. Roles and responsibilities

### 3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Agree to the terms on acceptable use of the school's ICT systems and the internet (appendices 1-3)

### 3.2 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

### 3.3 The designated safeguarding lead

Details of the school's DSL and deputy DSL are set out in our child protection policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- › Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- › Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board

This list is not intended to be exhaustive.

### **3.4 The ICT manager (a contracted, external support company)**

The ICT manager is responsible for:

- Ensuring that appropriate filtering and monitoring systems are in place, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Monitoring the school's ICT systems on an ongoing basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are reported to the DSL and dealt with appropriately
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

### **3.5 All staff and volunteers**

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 & 2)
- Working with the DSL to ensure that any online safety incidents are logged in accordance with the child protection policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Monitoring that devices are used for their intended educational purpose, by children
- Ensure that any digital content shared with pupils is age appropriate

This list is not intended to be exhaustive.

### **3.6 Parents**

Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 or 2)
- Discuss online safety with their children, developing confidence in children being able to share concerns
- Keep the school updated on permissions (such as photograph usage)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

› What are the issues? - [UK Safer Internet Centre](#)

› Hot topics - [Childnet International](#)

› Parent factsheet - [Childnet International](#)

### 3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

### 3.8 Children

Children are expected to

- Sign and adhere to the Acceptable Use agreement (appendices 1 or 2)
- Report any incidents of inappropriate material/behaviour, to an adult

## 4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum.

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

*By the **end of primary school**, pupils will know:*

- That people sometimes behave differently online, including by pretending to be someone they are not.
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

A comprehensive Computing scheme of work will be consistently delivered across the whole school, which will include specific work related to online safety.

The safe use of social media and the internet will also be covered in other subjects where relevant.

Children will be taught about their responsibility to be good online citizens and what this means.

The school will use assemblies to raise pupils' awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

## 5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents, via the school website (<http://www.lakeview.beds.sch.uk>).

Online safety will also be covered through an annual workshop for parents.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

## 6. Cyber-bullying

### 6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

### 6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with their classes, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

### 6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Any searching of pupils will be carried out in line with the DfE's latest guidance on [screening, searching and confiscation](#).

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

## **7. Acceptable use of the internet in school**

All pupils and staff sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2..

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action.

## **8. Pupils using mobile devices in school**

Pupils in years 4-6 may bring mobile phones into school, but are not permitted to use them during the day. They must hand them to the office, upon arrival and collect again upon departure.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

## **9. Staff using work devices outside school**

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 3.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school.

If staff have any concerns over the security of their device, they must seek advice from the ICT manager.

Work devices must be used solely activities necessary for the completion of the staff member's role.

## **10. How the school will respond to issues of misuse**

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

## **11. Training**

All new staff members are required to complete training, as part of their induction. This includes elements, on safe internet use, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

## **12. Monitoring arrangements**

The DSL logs behaviour and safeguarding issues related to online safety, using the schools safeguarding concern recording protocols. Online safety incidents are logged via the DSL (see appendix 4).

Governors are kept informed of developments through an annual report by the IT lead.

This policy will be reviewed every two years by the IT lead (or sooner if required). At every review, the policy will be shared with the governing board.

The IT managers monitor usage and raise any issues with the IT lead.

## **13. Links with other policies**

This online safety policy is linked to our:

- Child protection policy
- Behaviour policy
- Staff Code of Conduct
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure

**Date agreed: November 2023**


**Review date: November 2025**



## Appendix 1: acceptable use agreement Key Stage 1

This is how I keep **SAFE online**:

1. I only use the devices I'm **ALLOWED** to
2. I **CHECK** before I use new sites, games or apps
3. I **ASK** for help if I'm stuck
4. I **THINK** before I click
5. I **KNOW** people online aren't always who they say
6. I don't keep **SECRETS** just because someone asks me to
7. I don't change **CLOTHES** in front of a camera
8. I am **RESPONSIBLE** so never share private information
9. I am **KIND** and polite to everyone
10. I **TELL** a trusted adult if I'm worried, scared or just not sure
11. If I break the **RULES** I might not be allowed to use a computer / tablet



**My name is** \_\_\_\_\_ **Date** \_\_\_\_\_

## Appendix 2: acceptable use agreement Key Stage 2

1. I will only use **ICT** in school for schoolwork purposes.
2. I will **LOOK AFTER** school laptops and digital equipment and tell a teacher straight away if something is broken or not working properly.
3. I will keep my **LOGINS** and **PASSWORDS** to myself.
4. I will not attempt to visit websites or apps the school has **BLOCKED**.
5. I will not bring files into school without permission or **UPLOAD** inappropriate material to my workspace.
6. I will not **OPEN** an attachment, or **DOWNLOAD** a file, unless I know and trust the person who has it.
7. I will **ONLY EDIT OR DELETE MY OWN FILES** and not look at, or change, other people's files without their permission.
8. When in school I will only **CONTACT** people with my teacher's permission.
9. I will only **EMAIL** people I know or who are approved by my school.
10. I will not give my home address, phone number, send a photograph or video, or give any other **PERSONAL INFORMATION** that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
11. I will **NEVER ARRANGE TO MEET SOMEONE** I have only ever previously met on the internet.
12. I will hand in any personal **MOBILE DEVICE** to the school office on arrival and will make sure it is switched off.
13. I will not bring a **SMART WATCH** to school as they are not allowed to be worn during the school day.
14. I will be very careful when **SHARING** pictures or videos of myself or my friends. If I am in school I will always check with a teacher.
15. If I **SEE** anything I am unhappy with or I **RECEIVE** a message I do not like, I will not respond to it but I will immediately show a trusted adult.
16. I will make sure messages sent or information I upload, will always be **POLITE AND SENSIBLE**.
17. I understand that if I break the **RULES**, I may not be allowed to use digital equipment.


**I have read and understood these rules and agree to them.**

Name: \_\_\_\_\_

Class: \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

## Appendix 3: Lakeview School Acceptable Use Policy (Staff)

This policy covers use of all digital technologies while in school: i.e. **email, internet, intranet, network resources**, software, communication tools, social networking tools, school website, apps **and other relevant digital systems provided by the school.**

**It also covers school equipment when used outside of school, use of online systems provided by the school when accessed from outside school, and posts on social media made from outside school premises/hours which reference the school or which might bring your professional status into disrepute.**

The school systems and users are protected and monitored by security and filtering services to provide safe access to digital technologies. Your behaviour online when in school and on all school devices whether in school or otherwise may therefore be subject to monitoring.

- I will only use the school's digital technology resources and systems for professional purposes.
- I will not reveal my password(s) to anyone.
- I will follow 'good practice' advice in the creation and use of my password. If my password is compromised, I will ensure I change it.
- I will not use anyone else's password if they reveal it to me and will advise them to change it.
- I will not allow unauthorised individuals to access email / internet / intranet / network / social networks / mobile apps / or any other system I have access to via the school.
- I will ensure all documents, data, etc. are printed, saved, accessed and deleted / shredded in accordance with GDPR.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved email system(s) for any school business. This is currently: Office 365 – Outlook.
- I will only communicate with parents/carers in a professional manner and on appropriate school business, via the school office email, parentservices email, parent mail or the school phones.
- I will only communicate with pupils using a class Office 365 account, as part of the curriculum where necessary.
- I will not support or promote extremist organisations, messages or individuals.
- I will not give a voice or opportunity to extremist visitors with extremist views.
- I will not browse, download or send material that is illegal, considered offensive or of an extremist nature by the school.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach or equipment failure to the IT technician and computing leader.
- I will not download any software or resources from the internet that can compromise the network or might allow me to bypass the filtering and security system or that are not adequately licensed.
- I will check copyright and not publish, download or distribute any work including images, music and videos, that is protected by copyright, without seeking the author's permission.
- I will not connect any device to the network that does not have up-to-date anti-virus software, and I will keep any 'loaned' equipment up-to-date, using the school's anti-virus and ICT defence systems.
- I will not use personal digital cameras or camera phones or digital devices for taking, editing and transferring images or videos of pupils or staff.

- I will follow the school's policy on use of personal mobile phones and devices.
- I will only use school approved equipment for any storage, editing or transfer of digital images / videos and ensure I only save photographs and videos of children and staff on the staff drive within school.
- I will only take or publish images of staff and students with their permission and in accordance with the school's policy on the use of digital / video images. Images published on the school website, social media etc. will not identify students by name, or other personal information.
- I will ensure that any private social networking sites, blogs, etc. that I create or actively contribute to, are not confused with my professional role.
- I will ensure, where used, I know how to use any social networking sites' tools securely, so as not to compromise my professional role.
- I agree and accept that any device(s) loaned to me by the school, is provided solely to support my professional responsibilities.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I understand any information seen by me with regard to staff or pupils, held within the school's information management system, must be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I am aware that under the provisions of the GDPR (General Data Protection Regulation), my school and I have responsibilities regarding the creation, use, storage and deletion of data, and I will not store any pupil data that is not in line with the school's data policy and adequately protected.
- I understand it is my duty to support a whole-school safeguarding approach and will report any behaviour of other staff or pupils, which I believe may be inappropriate or concerning in any way, to the Designated Safeguarding Lead.
- I understand that all internet and network traffic / usage can be logged and this information can be made available *to the Head / Designated Safeguarding Lead* on their request.
- I understand that internet encrypted content (via the https protocol), may be scanned for security and/or safeguarding purposes.
- I understand that I have a responsibility to uphold the standing of the teaching profession and of the school, and that my digital behaviour can influence this.
- I agree to adhere to the Social Media and Mobile Phone Policy, set out by the school.
- *Staff that have a teaching role only:* I will embed the school's E Safety curriculum into my teaching.

**User Signature**

I agree to abide by all the points above.

I understand that failure to comply with this agreement could lead to disciplinary action or even legal interventions, depending on the seriousness of the incident.

Signature ..... Date.....

Full Name ..... (printed)

Job title / Role .....

## Appendix 4: Online Incident Record

Date	Pupils involved	Location of incident	Description of incident	Action taken (by whom)